

What is claimed is:

1           1.       A system for dynamically configuring parameterized validation  
2 rules in a distributed computing environment, comprising:  
3           a plurality of packet validation devices, each situated within the  
4 distributed computing environment at packet routing points and validating packet  
5 traffic using parameterized validation rules;  
6           a plurality of hierarchical tree nodes structured into a plurality of tiered  
7 layers with each tree node interfaced to at least one other tree node, those tree  
8 nodes at a lowermost layer further interfaced to at least one packet validation  
9 device from which validation rule parameters are retrieved and processed; and  
10          a root tree node interfaced to an uppermost layer of tree nodes from which  
11 validation rule parameters are retrieved and disseminated to each of the packet  
12 validation devices.

1           2.       A system according to Claim 1, further comprising:  
2           a concast path interconnecting the packet validation devices, the tree  
3 nodes, and the root tree node via an interconnection reserved for validation rule  
4 parameter exchange.

1           3.       A system according to Claim 1, further comprising:  
2           a dissemination path interconnecting the root tree node with each packet  
3 validation device via a interconnection reserved for validation rule parameter  
4 exchange.

1           4.       A system according to Claim 1, further comprising:  
2           a filter executed by each tree node on retrieved validation rule parameters  
3 to remove at least one of duplicate validation rule parameters and validation rule  
4 parameters sharing commonly identified network address space.

1           5.       A system according to Claim 1, wherein the validation rule  
2 parameters each comprise a source network address and subnet mask, a source



1           10.    A method according to Claim 6, wherein the validation rule  
2 parameters each comprise a source network address and subnet mask, a source  
3 network port, a destination network address and subnet mask, a destination  
4 network port, and one or more network protocol identifiers.

1           11.    A computer-readable storage medium holding code for performing  
2 the method of Claim 6.

1           12.    A system for communicating coalesced rule parameters in a  
2 distributed computing environment, comprising:  
3           a plurality of packet validation devices communicatively interposed  
4 between network routing points within the distributed computing environment  
5 and applying parameterized rules to transiting network packet traffic;  
6           a plurality of processing tree nodes configured into a concast tree,  
7 comprising:  
8                 in a lowermost layer of the concast tree, each processing tree node  
9 collecting and coalescing rule parameters from at least one packet validation  
10 device; and  
11                in each successive layer of the concast tree, each processing tree  
12 node collecting and coalescing the rule parameters from at least one processing  
13 tree node in a next lower layer of the concast tree;  
14           a control center assembling the coalesced rule parameters from each  
15 packet validation device in an uppermost layer of the concast tree; and  
16           a dissemination path forwarding the coalesced rule parameters from the  
17 control center to each packet validation device.

1           13.    A system according to Claim 12, wherein each processing tree  
2 node further comprises:  
3           a parameter filter removing duplicate rule parameters and consolidating  
4 commonly identified network address space.



6 destination packet information describing a destination network address  
7 and subnet mask;  
8 destination port information describing a destination network port; and  
9 network protocol information identifying one or more network protocols.

1 20. A system according to Claim 12, wherein the distributed  
2 computing environment comprises an internet-protocol (IP)-based network.

1 21. A method for communicating coalesced rule parameters in a  
2 distributed computing environment, comprising:  
3 applying parameterized rules to network packet traffic transiting a  
4 plurality of packet validation devices communicatively interposed between  
5 network routing points within the distributed computing environment;  
6 configuring a plurality of processing tree nodes into a concast tree,  
7 comprising:  
8 collecting and coalescing rule parameters from at least one packet  
9 validation device into a processing tree node in a lowermost layer of the concast  
10 tree; and  
11 collecting and coalescing the rule parameters from at least one  
12 processing tree node in a next lower layer of the concast tree in each successive  
13 layer of the concast tree;  
14 assembling the coalesced rule parameters from each packet validation  
15 device in an uppermost layer of the concast tree into a control center and  
16 forwarding the assembled coalesced rule parameters to each packet validation  
17 device.

1 22. A method according to Claim 21, further comprising:  
2 removing duplicate rule parameters and consolidating commonly  
3 identified network address space.

1 23. A method according to Claim 21, further comprising

2 limiting application of the coalesced rule parameters to those network  
3 routing points within a pre-determined vicinity.

1 24. A method according to Claim 21, further comprising:  
2 broadcasting the assembled coalesced rule parameters through the  
3 distributed computing environment to each packet validation device.

1 25. A method according to Claim 21, further comprising:  
2 sending the assembled coalesced rule parameters to each packet validation  
3 device through the concast tree via the processing tree nodes.

1 26. A method according to Claim 21, further comprising:  
2 logically defining an in-band communication channel by reserving  
3 bandwidth within the distributed computing environment.

1 27. A method according to Claim 21, wherein the concast tree further  
2 comprises:  
3 interfacing the packet validation devices, the processing tree nodes, and  
4 the control center via an out-of-band communication channel using  
5 interconnections peripheral to the distributed computing environment.

1 28. A method according to Claim 21, wherein the rule parameters each  
2 comprise:  
3 source packet information describing a source network address and subnet  
4 mask;  
5 source port information describing a source network port;  
6 destination packet information describing a destination network address  
7 and subnet mask;  
8 destination port information describing a destination network port; and  
9 network protocol information identifying one or more network protocols.

1 29. A method according to Claim 21, wherein the distributed  
2 computing environment comprises an internet-protocol (IP)-based network.

